

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

KRISTI JORDAN, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

CRUNCH, LLC,

Defendant.

Civil Action No. 1:24-cv-7118

CLASS ACTION

DEMAND FOR JURY TRIAL

FIRST AMENDED CLASS ACTION COMPLAINT

INTRODUCTION

Kristi Jordan (“Plaintiff”), individually and on behalf of all others similarly situated, makes the following allegations pursuant to the investigation of counsel and based upon information and belief, except as to allegations pertaining specifically to herself or her counsel, which are based on personal knowledge.

NATURE OF THE CASE

1. Plaintiff brings this action to redress Defendant Crunch LLC’s (“Defendant”) practice of knowingly disclosing Plaintiff’s and its other customers’ identities and the titles of prerecorded video materials to which they have purchased access to Meta Platforms, Inc. (“Meta”), formerly known as Facebook, Inc. (“Facebook”), in violation of the federal Video Privacy Protection Act (“VPPA”), 18 U.S.C. § 2710.

2. Over the past two years, Defendant has systematically transmitted (and continues to transmit today) its customers’ personally identifying video viewing information to Meta using a snippet of programming code called the “Meta Pixel,” which Defendant installed and configured on its www.crunchplus.com website (the “Website”).

3. The information Defendant disclosed (and continues to disclose) to Meta via the Meta Pixel includes the customer’s Facebook ID (“FID”) and the title of the specific prerecorded video material that each of its customers watched on its Website. It also includes the customer’s FID and the fact that the customer purchased a

subscription to Defendant's Website. An FID is a unique sequence of numbers linked to a specific Meta profile. A Meta profile, in turn, identifies by name the specific person to whom the profile belongs (and also contains other personally identifying information about the person). Entering "Facebook.com/[FID]" into a web browser returns the Meta profile of the person to whom the FID corresponds. Thus, the FID identifies a person more precisely than a name, as numerous persons may share the same name, but each person's Facebook profile (and associated FID) uniquely identifies one and only one person. In the simplest terms, the Meta Pixel installed by Defendant captures and discloses to Meta information that reveals the specific videos that a particular person watched through a paid subscription on Defendant's Website (hereinafter, "Private Viewing Information").

4. Defendant disclosed and continues to disclose its customers' Private Viewing Information to Meta without asking for, let alone obtaining, their consent to these practices.

5. The VPPA clearly prohibits what Defendant has done. Subsection (b)(1) of the VPPA provides that, absent the consumer's prior informed, written consent, any "video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for," 18 U.S.C. § 2710(b)(1), damages in the amount of \$2,500.00, *see id.* § 2710(c).

6. Accordingly, on behalf of herself and the putative Class members defined below, Plaintiff brings this Class Action Complaint against Defendant for intentionally and unlawfully disclosing her Personal Viewing Information to Meta.

PARTIES

I. Plaintiff Kristi Jordan

7. Plaintiff is, and at all times relevant hereto was, a citizen and resident of Tarrant County, Texas.

8. Plaintiff has used and continues to use the same device to maintain and access an active Facebook account throughout the relevant period in this case.

9. Plaintiff has purchased a monthly subscription to Defendant's Website which provides access to prerecorded video materials. Among other times, Plaintiff paid for this monthly subscription on September 11, 2024. Plaintiff provided her name, email address, and home address in association with the purchase of this subscription. Accordingly, Plaintiff requested or obtained, and is therefore a consumer of, prerecorded video material sold by Defendant on its Website.

10. At all times relevant hereto, including when purchasing subscription access to prerecorded video material from Defendant on its Website, Plaintiff had a Meta account, a Meta profile, and an FID associated with such profile.

11. Plaintiff has watched prerecorded videos on Defendant's Website through her paid subscription while logged into Facebook during the last two years.

12. When Plaintiff purchased a subscription from Defendant and viewed

prerecorded videos on its Website through the use of that subscription, Defendant disclosed to Meta Plaintiff's FID coupled with the specific title of the video she purchased (as well as the URL where such video is available for purchase), among other information about Plaintiff and the device she used to make the purchase.

13. Plaintiff has never consented, agreed, authorized, or otherwise permitted Defendant to disclose her Private Viewing Information to Meta. In fact, Defendant has never even provided Plaintiff with written notice of its practices of disclosing its customers' Private Viewing Information to third parties such as Meta.

14. Because Defendant disclosed Plaintiff's Private Viewing Information (including her FID, the title of the prerecorded video material she viewed through her subscription to Defendant's Website, and the URL where such video is available for viewing) to Meta during the applicable statutory period, Defendant violated Plaintiff's rights under the VPPA and invaded her statutorily conferred interest in keeping such information (which bears on her personal affairs and concerns) private.

II. Defendant Crunch, LLC

15. Defendant Crunch, LLC is a Delaware limited liability company with a principal place of business at P.O. Box 1918, Old Chelsea Station, New York, NY 10011.

JURISDICTION AND VENUE

16. The Court has subject-matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2710.

17. Personal jurisdiction and venue are proper because Defendant maintains its headquarters and principal place of business in Manhattan, New York within this judicial District.

VIDEO PRIVACY PROTECTION ACT

18. The VPPA prohibits companies (like Defendant) from knowingly disclosing to third parties (like Meta) information that personally identifies consumers (like Plaintiff) as having viewed particular videos or other audio-visual materials.

19. Specifically, subject to certain exceptions that do not apply here, the VPPA prohibits “a video tape service provider” from “knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider[.]” 18 U.S.C. § 2710(b)(1). The statute defines a “video tape service provider” as “any person, engaged in the business . . . of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials,” 18 U.S.C. § 2710(a)(4). It defines a “consumer” as “a renter, purchaser, or subscriber of goods or services from a video tape service provider.” 18 U.S.C. § 2710(a)(1). “[P]ersonally identifiable information’ includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.” 18 U.S.C. § 2710(a)(3).

20. Leading up to the VPPA’s enactment in 1988, members of the United States Senate warned that “[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that

information goes.” S. Rep. No. 100-599 at 7-8 (1988) (statements of Sen. Simon). Senators at the time were particularly troubled by disclosures of records that reveal consumers’ purchases and rentals of videos and other audiovisual materials because such records offer “a window into our loves, likes, and dislikes,” such that “the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance.” *Id.* at 8 (statement of Sen. Leahy).

21. Thus, in proposing the Video and Library Privacy Protection Act (which later became the VPPA), Senator Patrick J. Leahy (the senior Senator from Vermont from 1975 to 2023) sought to codify, as a matter of law, that “our right to privacy protects the choice of movies that we watch with our family in our own homes.” 134 Cong. Rec. S5399 (May 10, 1988). As Senator Leahy explained at the time, the personal nature of such information, and the need to protect it from disclosure, is the *raison d’être* of the statute: “These activities are at the core of any definition of personhood. They reveal our likes and dislikes, our interests and our whims. They say a great deal about our dreams and ambitions, our fears and our hopes. They reflect our individuality, and they describe us as people.” *Id.*

22. While these statements rang true in 1988 when the act was passed, the importance of legislation like the VPPA in the modern era of data mining is more pronounced than ever before. During a more recent Senate Judiciary Committee meeting, “The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st

Century,” Senator Leahy emphasized the point by stating: “While it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the ‘cloud,’ mobile apps and other new technologies have revolutionized the availability of Americans’ information.”¹

23. Former Senator Al Franken may have said it best: “If someone wants to share what they watch, I want them to be able to do so . . . But I want to make sure that consumers have the right to easily control who finds out what they watch—and who doesn’t. The Video Privacy Protection Act guarantees them that right.”²

24. In this case, however, Defendant deprived Plaintiff and numerous other similarly situated persons of that right by systematically (and surreptitiously) disclosing their Private Viewing Information to Meta, without providing notice to (let alone obtaining consent from) any of them, as explained in detail below.

¹ The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century, Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, <http://www.judiciary.senate.gov/meetings/the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21stcentury>.

² Chairman Franken Holds Hearing on Updated Video Privacy Law for 21st Century, franken.senate.gov (Jan. 31, 2012).

BACKGROUND FACTS

I. Consumers' Personal Information Has Real Market Value

25. In 2001, Federal Trade Commission ("FTC") Commissioner Orson Swindle remarked that "the digital revolution . . . has given an enormous capacity to the acts of collecting and transmitting and flowing of information, unlike anything we've ever seen in our lifetimes . . . [and] individuals are concerned about being defined by the existing data on themselves."³

26. Over two decades later, Commissioner Swindle's comments ring truer than ever, as consumer data feeds an information marketplace that supports a 26 billion dollar per year online advertising industry in the United States.⁴

27. The FTC has also recognized that consumer data possesses inherent monetary value within the new information marketplace and publicly stated that:

Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.⁵

³ Transcript, *The Information Marketplace* (Mar. 13, 2001), at 8-11, available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

⁴ See Julia Angwin and Emily Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011), available at <https://www.wsj.com/articles/SB10001424052748703529004576160764037920274>.

⁵ Statement of FTC Cmr. Harbour (Dec. 7, 2009), at 2, available at https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf

28. In fact, an entire industry exists while companies known as data aggregators purchase, trade, and collect massive databases of information about consumers. Data aggregators then profit by selling this “extraordinarily intrusive” information in an open and largely unregulated market.⁶

29. The scope of data aggregators’ knowledge about consumers is immense: “If you are an American adult, the odds are that [they] know[] things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams—and on and on.”⁷

30. Further, “[a]s use of the Internet has grown, the data broker industry has already evolved to take advantage of the increasingly specific pieces of information about consumers that are now available.”⁸

31. Recognizing the severe threat the data mining industry poses to consumers’ privacy, on July 25, 2012, the co-chairmen of the Congressional Bi-Partisan Privacy Caucus sent a letter to nine major data brokerage companies seeking

⁶ See M. White, *Big Data Knows What You’re Doing Right Now*, TIME.com (July 31, 2012), available at <http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/>.

⁷ N. Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y. Times (June 16, 2012), available at <https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html#:~:text=It's%20called%20the%20Acxiom%20Corporation,to%20know%20much%2C%20much%20more>.

⁸ Letter from Sen. J. Rockefeller IV, Sen. Cmtee. On Commerce, Science, and Transportation, to S. Howe, Chief Executive Officer, Acxiom (Oct. 9, 2012) available at <https://www.commerce.senate.gov/services/files/3bb94703-5ac8-4157-a97b-%20a658c3c3061c>.

information on how those companies collect, store, and sell their massive collections of consumer data, stating in pertinent part:

By combining data from numerous offline and online sources, data brokers have developed hidden dossiers on every U.S. consumer. This large[-]scale aggregation of the personal information of hundreds of millions of American citizens raises a number of serious privacy concerns.⁹

32. Data aggregation is especially troublesome when consumer information is sold to direct-mail advertisers. In addition to causing waste and inconvenience, direct-mail advertisers often use consumer information to lure unsuspecting consumers into various scams, including fraudulent sweepstakes, charities, and buying clubs. Thus, when companies like Defendant share information with data aggregators, data cooperatives, and direct-mail advertisers, they contribute to the “[v]ast databases” of consumer data that are often “sold to thieves by large publicly traded companies,” which “put[s] almost anyone within the reach of fraudulent telemarketers” and other criminals.¹⁰

33. Disclosures like Defendant’s are particularly dangerous to the elderly. “Older Americans are perfect telemarketing customers, analysts say, because they are

⁹ See *Bipartisan Group of Lawmakers Query Data Brokers About Practices Involving Consumers’ Personal Information*, Website of Sen. Markey (July 24, 2012), available at <https://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-brokers-about-practices-involving-consumers-personal-information>.

¹⁰ See Charles Duhigg, *Bilking the Elderly, with a Corporate Assist*, N.Y. Times (May 20, 2007), available at <https://www.nytimes.com/2007/05/20/business/20tele.html>.

often at home, rely on delivery services, and are lonely for the companionship that telephone callers provide.”¹¹

34. The FTC notes that “[t]he elderly often are the deliberate targets of fraudulent telemarketers who take advantage of the fact that many older people have cash reserves or other assets to spend on seemingly attractive offers.”¹²

35. Indeed, an entire black market exists while the personal information of vulnerable elderly Americans is exchanged. Thus, information disclosures like Defendant’s are particularly troublesome because of their cascading nature: “Once marked as receptive to [a specific] type of spam, a consumer is often bombarded with similar fraudulent offers from a host of scam artists.”¹³

36. Defendant is not alone in violating its customers’ statutory rights and jeopardizing their well-being in exchange for increased revenue: disclosing customer and subscriber information to data aggregators, data appenders, data cooperatives, direct marketers, and other third parties has become a widespread practice. Unfortunately for consumers, however, this growth has come at the expense of their most basic privacy rights.

¹¹ *Id.*

¹² Prepared Statement of the FTC on “Fraud Against Seniors” before the Special Committee on Aging, United States Senate (August 10, 2000).

¹³ *Id.*

II. Consumers Place Monetary Value on Their Privacy and Consider Privacy Practices When Making Purchases

37. As the data aggregation industry has grown, so has consumer concerns regarding personal information.

38. A survey conducted by Harris Interactive on behalf of TRUSTe, Inc. showed that 89 percent of consumers polled avoid doing business with companies who they believe do protect their privacy online.¹⁴ As a result, 81 percent of smartphone users polled said that they avoid using smartphone apps that they don't believe protect their privacy online.¹⁵

39. Thus, as consumer privacy concerns grow, consumers increasingly incorporate privacy concerns and values into their purchasing decisions, and companies viewed as having weaker privacy protections are forced to offer greater value elsewhere (through better quality and/or lower prices) than their privacy-protective competitors. In fact, consumers' personal information has become such a valuable commodity that companies are beginning to offer individuals the opportunity to sell their personal information themselves.¹⁶

¹⁴ See 2014 TRUSTe US Consumer Confidence Privacy Report, TRUSTe, http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf.

¹⁵ *Id.*

¹⁶ See Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. Times (Feb. 12, 2012), available at <https://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html>.

40. These companies' business models capitalize on a fundamental tenet underlying the personal information marketplace: consumers recognize the economic value of their private data. Research shows that consumers are willing to pay a premium to purchase services from companies that adhere to more stringent policies of protecting their personal data.¹⁷

41. Thus, in today's digital economy, individuals and businesses alike place a real, quantifiable value on consumer data and corresponding privacy rights.¹⁸ As such, where a business offers customers a product or service that includes statutorily guaranteed privacy protections, yet fails to honor these guarantees, the customer receives a product or service of less value than the product or service paid for.

III. Defendant Uses the Meta Pixel to Systematically Disclose its Customers' Private Viewing Information to Meta

42. As alleged below, whenever a person with a Meta account views prerecorded video material on Defendant's Website through that person's paid subscription, the Meta Pixel technology that Defendant intentionally installed on its Website transmits the customer's personally identifying information and detailed

¹⁷ See Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (2011); see also European Network and Information Security Agency, *Study on Monetizing Privacy* (Feb. 27, 2012), available at <https://www.enisa.europa.eu/publications/monetising-privacy>.

¹⁸ See Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2003) at 2, available at <https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf>.

Private Viewing Information (revealing the specific titles of the prerecorded video material that he or she purchased) to Meta – all without the customer’s consent, and in clear violation of the VPPA. The Meta Pixel technology also reveals that a consumer has purchased a subscription to access prerecorded video content on Defendant’s website alongside that consumer’s personally identifying information.

A. The Meta Pixel

43. On February 4, 2004, Mark Zuckerberg and others launched Facebook, now known as “Meta.”¹⁹ Meta is now the world’s largest social media platform. To create a Meta account, a person must provide, *inter alia*, his or her first and last name, birth date, gender, and phone number or email address.

44. The Meta Pixel, first introduced in 2013 as the “Facebook Pixel,” is a unique string of code that companies can embed on their websites to monitor and track the actions taken by visitors to their websites and to report them back to Meta. This allows companies like Defendant to build detailed profiles about their customers and to serve them with highly targeted advertising.

45. Additionally, a Meta Pixel installed on a company’s website allows Meta to “match [] website visitors to their respective Facebook User accounts.”²⁰ This is because Meta has assigned to each of its users an “FID” number – a unique

¹⁹ See Facebook, “Company Info,” available at <https://about.fb.com/company-info/>.

²⁰ Meta, “Get Started – Meta Pixel,” available at <https://developers.facebook.com/docs/meta-pixel/get-started/>.

and persistent identifier that allows anyone to look up the user's unique Meta profile and thus identify the user by name²¹ – and because each transmission of information made from a company's website to Meta via the Meta Pixel is accompanied by, *inter alia*, the FID of the website's visitor. Moreover, the Meta Pixel can follow a consumer to different websites and across the Internet even after the consumer's browser history has been cleared.

46. Meta has used the Meta Pixel to amass a vast digital database of dossiers comprised of highly detailed personally identifying information about each of its billions of users worldwide, including information about all of its users' interactions with any of the millions of websites across the Internet on which the Meta Pixel is installed. Meta then monetizes this Orwellian database by selling advertisers the ability to serve highly targeted advertisements to the persons whose personal information is contained within it.

47. Simply put, if a company chooses to install the Meta Pixel on its website, both the company who installed it and Meta (the recipient of the information it transmits) are then able to “track [] the people and type of actions they

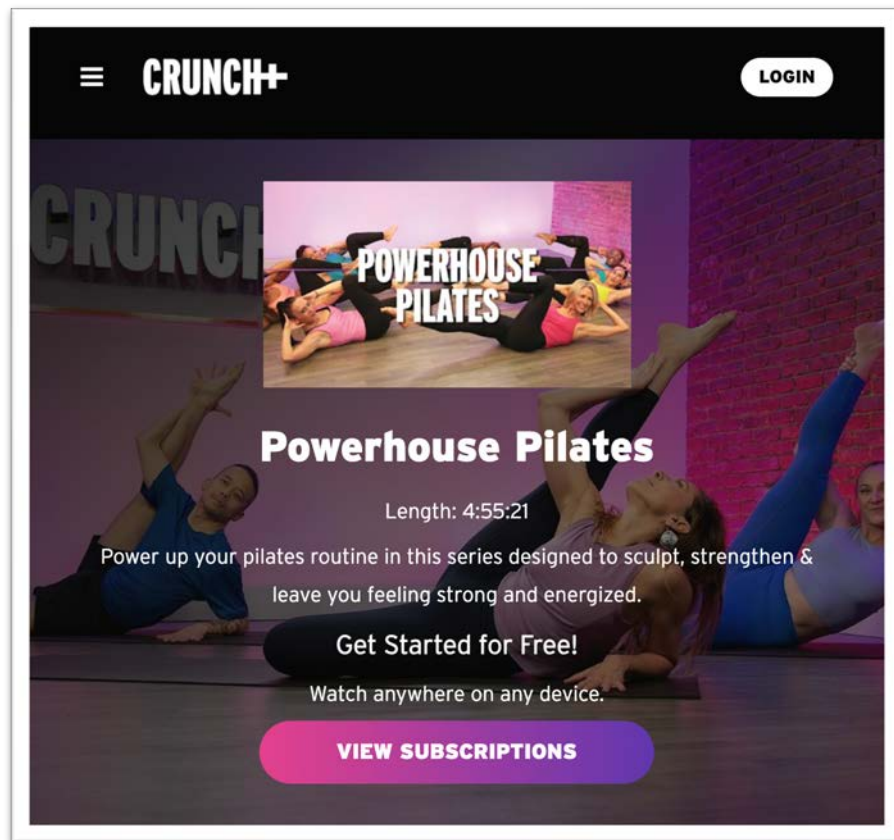
²¹ For example, Mark Zuckerberg's FID is reportedly the number “4,” so logging into Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck, and all of the additional personally identifiable information contained therein.

take,”²² including, as relevant here, the specific prerecorded video material that they purchase on the website.

B. Defendant Knowingly Uses the Meta Pixel to Transmit the Private Viewing Information of its Customers to Meta

48. Defendant sells access to prerecorded video materials to consumers on the Website (www.crunchplus.com).

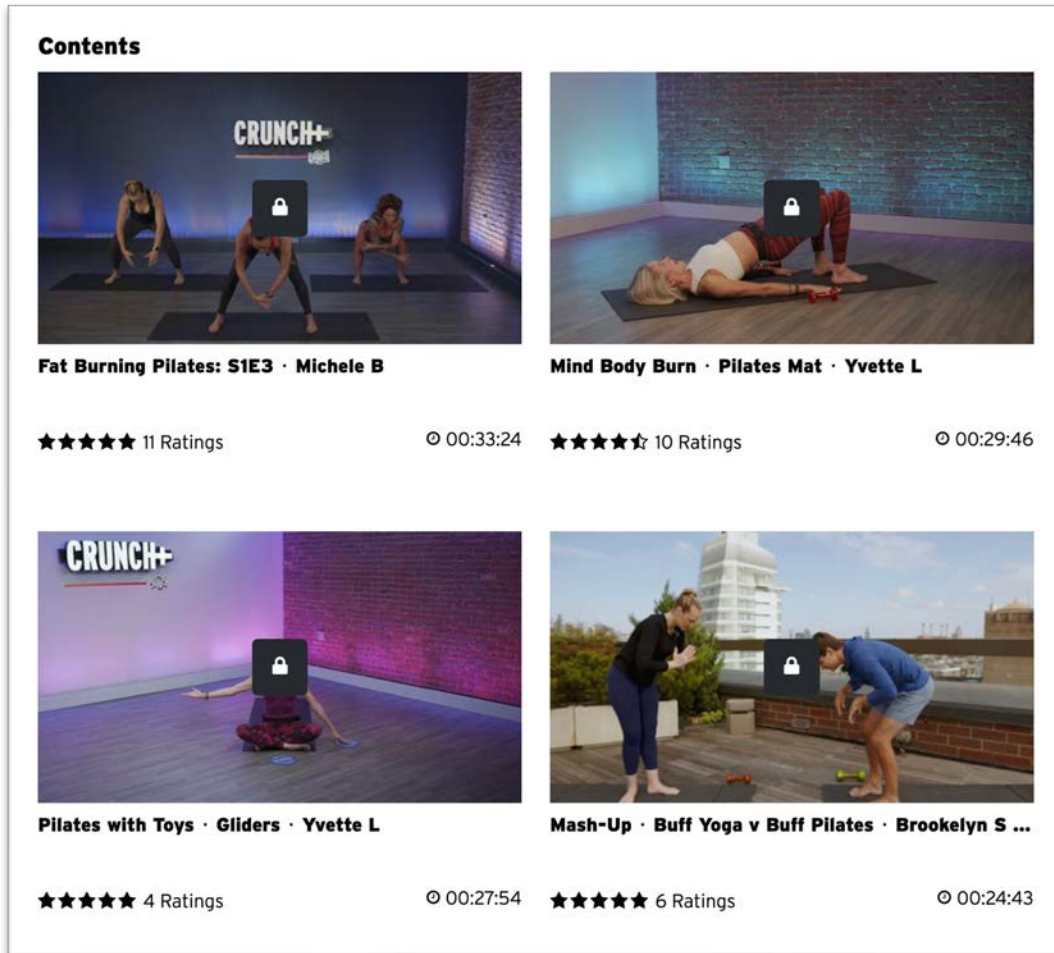
49. These video materials include numerous instructional exercise videos, as shown in the screenshot example below from the Website.²³



²² Meta, “Retargeting: How to Advertise to Existing Customers with Ads on Facebook,” available at https://www.facebook.com/business/goals/retargeting?checkpoint_src=any.

²³ Crunch, “Powerhouse Pilates,” available at <https://www.crunchplus.com/products/powerhouse-pilates>.

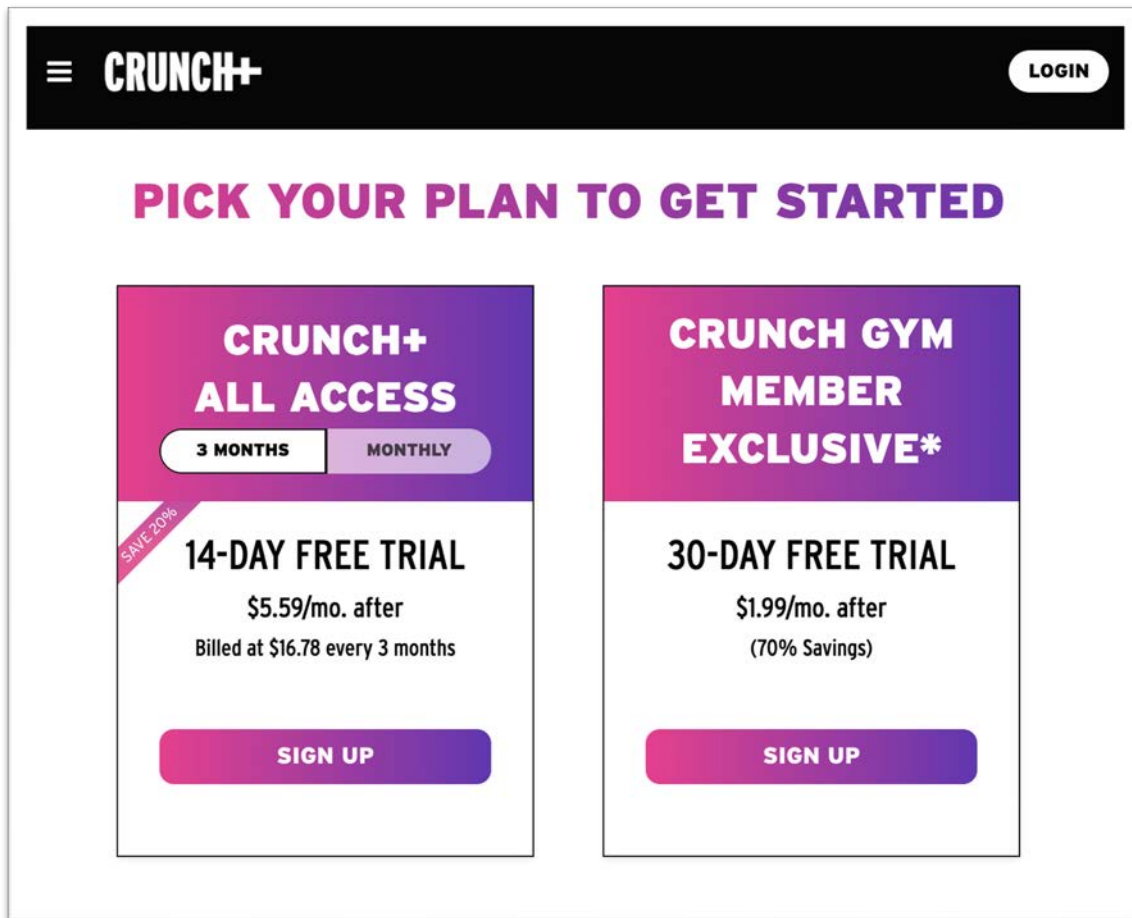
50. These videos on Defendant's Website are only available to subscribers. This is indicated by the "lock" insignias displayed over previews of the videos on the following screenshot.²⁴



51. Defendant offers multiple paid subscription tiers which permit consumers to access these videos, as pictured in the screenshot presented below.²⁵

²⁴ *Id.*

²⁵ Crunch, "Crunch+ By Crunch Fitness," available at https://www.crunchplus.com/crunch_subscriptions.



52. To buy a subscription providing access to the prerecorded video materials on Defendant's Website, a person must provide at least his or her name, email address, billing address, and credit or debit card (or other form of payment) information.

53. Whenever a person with a Meta account purchases a subscription to view prerecorded video materials on the Website, Defendant uses – and has used at all times relevant hereto – the Meta Pixel to disclose to Meta the unencrypted FID of the person who made the purchase as well as the fact that the person is purchasing requesting or obtaining video material from Defendant.

54. Furthermore, whenever a person with a Meta account logs into his or her account on Defendant’s Website (obtained through purchasing a subscription) and watches a prerecorded video, Defendant uses – and has used at all times relevant hereto – the Meta Pixel to disclose to Meta the unencrypted FID of the person who watched the video, the URL of the webpage containing the video, and the name of the video the person watched.

55. The URL of each webpage containing a prerecorded video on Defendant’s website includes the name of the video hosted on that page.

56. For example, one video hosted on Defendant’s website is entitled “Brazilian Body Blast.” The title “Brazilian Body Blast” is included in the URL of the page hosting that video,²⁶ as is true of all webpages hosting videos on Defendant’s Website.

57. Each video accessible on Defendant’s Website is hosted on a dedicated webpage with no other videos available to stream on that page.

58. In these ways, among other methods, Defendant knowingly discloses to Meta the Private Viewing Information of its consumers. Specifically, when consumers watch prerecorded videos on Defendant’s Website, the Website executes a GET request to Facebook’s tracking URL “https://www.facebook.com/tr” and sends it querystring parameters and cookie values which disclose the name of the

²⁶ The URL for the page hosting the “Brazilian Body Blast” video is <https://www.crunchplus.com/assets/brazilian-body-blast?autoplay=true&progress=0&filters=false&category=%22Crunch%20Classic%22>.

videos watched by the consumer, the URLs of the webpages hosting the videos, and the consumer's FID.

59. Plaintiff has purchased a subscription to Defendant's Website while logged into Facebook during the last two years. Accordingly, Defendant has transmitted Plaintiff's identity and the fact that she requested or obtained a subscription to access prerecorded video material to Meta during the last two years.

60. Plaintiff has watched a prerecorded video on Defendant's Website through her paid subscription while logged into Facebook during the last two years. Accordingly, Defendant transmitted Plaintiff's identity, the title of the videos she watched, and the URLs to Meta during the last two years.

61. Defendant intentionally programmed its Website to include the Meta Pixel code in order to take advantage of the targeted advertising and other informational and analytical services offered by Meta.

62. The Meta Pixel code systematically transmits to Meta the FID of each person with a Meta account who watches prerecorded video material on its Website, along with the specific title of the prerecorded video material that the person watched through a paid subscription.

63. The Meta Pixel code systematically transmits to Meta the FID of each person with a Meta account who purchases a subscription to prerecorded video material on its Website, along with fact that the person purchased a paid subscription.

64. With only a person's FID and the title of the prerecorded video material watched (or URL where such material is available)—all of which Defendant knowingly provides to Meta on a systematic basis—any ordinary person could learn the identity of the person to whom the FID corresponds and identify the specific prerecorded video material that the person purchased or watched (and thus requested and obtained). The person's identity can be determined by simply by accessing the URL [www.facebook.com/\[insert the person's FID here\]/](http://www.facebook.com/[insert the person's FID here]/).

65. With only a person's FID and the fact that the person purchased a subscription to the Defendant's Website—all of which Defendant knowingly provides to Meta on a systematic basis—any ordinary person could learn the identity of the person to whom the FID corresponds and identify the prerecorded video materials that the person requested and obtained. The person's identity can be determined by simply by accessing the URL [www.facebook.com/\[insert the person's FID here\]/](http://www.facebook.com/[insert the person's FID here]/).

66. Defendant's practices of disclosing the Private Viewing Information of its customers to Meta continued unabated for the duration of the two-year period preceding the filing of this action.

67. At all times relevant hereto, whenever Plaintiff or any other person purchased or watched prerecorded video material on Defendant's Website, Defendant disclosed to Meta (*inter alia*) the specific title of the video material that was purchased or watched (including the URL where such material is available for purchase), along

with the FID of the person who purchased or watched it (which, as discussed above, uniquely identified the person).

68. At all times relevant hereto, whenever Plaintiff or any other person purchased a paid subscription from Defendant on its Website, Defendant disclosed to Meta (*inter alia*) the fact that the person purchased a subscription (including the URL where such a subscription is available for purchase), along with the FID of the person who purchased it (which, as discussed above, uniquely identified the person).

69. At all times relevant hereto, Defendant knew that the Meta Pixel was disclosing its customers' Private Viewing Information to Meta.

70. Although Defendant could easily have programmed its Website so that none of its customers' Private Viewing Information is disclosed to Meta, Defendant instead chose to program its Website so that all of its customers' Private Viewing Information is disclosed to Meta.

71. Before transmitting its customers' Private Viewing Information to Meta, Defendant failed to notify any of them that it would do so, and none of them have ever consented (in writing or otherwise) to these practices.

72. By intentionally disclosing to Meta Plaintiff's and its other customers' FIDs together with the specific video material that they each watched or the fact that they purchased a subscription, without any of their consent to these practices, Defendant knowingly violated the VPPA on an enormous scale.

CLASS ACTION ALLEGATIONS

73. Plaintiff seeks to represent a class defined as all persons in the United States who, during the two years preceding the filing of this action, requested or obtained video content as a subscriber to Defendant's Website while maintaining an account with Meta Platforms, Inc. f/k/a Facebook, Inc.

74. Class members are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class number in at least the tens of thousands. The precise number of Class members and their identities are unknown to Plaintiff at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the membership records of Defendant.

75. Common questions of law and fact exist for all Class members and predominate over questions affecting only individual class members. Common legal and factual questions include but are not limited to (a) whether Defendant embedded Meta Pixel on its Website that monitors and tracks actions taken by visitors to its Website; (b) whether Defendant reports the actions and information of visitors to Meta; (c) whether Defendant knowingly disclosed Plaintiff's and Class members' Private Viewing Information to Meta; (d) whether Defendant's conduct violates the Video Privacy Protection Act, 18 U.S.C. § 2710; and (e) whether Plaintiff and Class members is entitled to a statutory damage award of \$2,500, as provided by the VPPA.

76. The named Plaintiff's claims are typical of the claims of the Class in that the Defendant's conduct toward the putative class is the same. That is, Defendant embedded Meta Pixel on its Website to monitor and track actions taken by class members to its Website and report this to Meta. Further, the named Plaintiff and the Class members suffered invasions of their statutorily protected right to privacy (as afforded by the VPPA), as well as intrusions upon their private affairs and concerns that would be highly offensive to a reasonable person, as a result of Defendant's uniform and wrongful conduct in intentionally disclosing their Private Viewing Information to Meta.

77. Plaintiff is an adequate representative of the Class because she is interested in the litigation; her interests do not conflict with those of the Class members she seeks to represent; she has retained competent counsel experienced in prosecuting class actions and intends to prosecute this action vigorously. Plaintiff and her counsel will fairly and adequately protect the interests of all Class members.

78. The class mechanism is superior to other available means for the fair and efficient adjudication of Class members' claims. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by this case's complex legal and factual issues. Individualized litigation also presents a potential for inconsistent or

contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication of the common questions of law and fact, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

CAUSE OF ACTION

Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710

79. Plaintiff repeats the allegations asserted in the preceding paragraphs as if fully set forth herein.

80. The VPPA prohibits a “video tape service provider” from knowingly disclosing “personally identifying information” concerning any “consumer” to a third party without the “informed, written consent (including through an electronic means using the Internet) of the consumer.” 18 U.S.C. § 2710.

81. As defined in 18 U.S.C. § 2710(a)(4), a “video tape service provider” is “any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials[.]” Defendant is a “video tape service provider” as defined in 18 U.S.C. § 2710(a)(4) because it is engaged in the business of selling and delivering prerecorded video materials, similar to prerecorded video cassette tapes, to consumers nationwide.

82. As defined in 18 U.S.C. § 2710(a)(1), a “‘consumer’ means any renter, purchaser, or consumer of goods or services from a video tape service provider.” As alleged above, Plaintiff and each of the Class members are a “consumer” within the meaning of the VPPA because they each purchased a subscription to access prerecorded video material or purchased prerecorded video material from Defendant’s Website that was sold and delivered to them by Defendant.

83. As defined in 18 U.S.C. § 2710(a)(3), “‘personally identifiable information’ includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.” The Private Viewing Information that Defendant transmitted to Meta constitutes “personally identifiable information” as defined in 18 U.S.C. § 2710(a)(3) because it identified Plaintiff and the Class members to Meta as an individual who purchased, and thus “requested or obtained,” specific prerecorded video material or a subscription to access prerecorded video material from Defendant via its Website.

84. Defendant knowingly disclosed Plaintiff’s and Class members’ Private Viewing Information to Meta via the Meta Pixel technology because Defendant intentionally installed and programmed the Meta Pixel code on its Website, knowing that such code would transmit to Meta the titles of the video materials watched by its customers coupled with its customers’ unique identifiers (including FIDs).

85. Defendant further knowingly disclosed Plaintiff’s and Class members’ Private Viewing Information to Meta via the Meta Pixel technology because

Defendant intentionally installed and programmed the Meta Pixel code on its Website, knowing that such code would transmit to Meta the subscriptions purchased and the specific prerecorded video material requested or obtained by its customers coupled with its customers' unique identifiers (including FIDs).

86. Defendant failed to obtain informed written consent from Plaintiff or any of the Class members authorizing it to disclose their Private Viewing Information to Meta or any other third party. More specifically, at no time prior to or during the applicable statutory period did Defendant obtain from any person who purchased prerecorded video material on its Website (including Plaintiff or any of the Class members) informed, written consent that was given in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer, that was given at the time the disclosure is sought or was given in advance for a set period of time, not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner, or that was given after Defendant provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw consent on a case-by-case basis or to withdraw consent from ongoing disclosures, at the consumer's election. *See* 18 U.S.C. § 2710(b)(2).

87. By disclosing Plaintiff's and Class members' Private Viewing Information, Defendant violated their statutorily protected right to privacy in their Private Viewing Information.

88. Consequently, Defendant is liable to Plaintiff and each of the Class members for damages in the statutorily set sum of \$2,500. 18 U.S.C. § 2710(c)(2)(A).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks a judgment against Defendant Crunch, LLC as follows:

- a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;
- b) For an order declaring that Defendant's conduct as described herein violated the VPPA;
- c) For an order finding in favor of Plaintiff and the Class and against Defendant on all counts asserted herein;
- d) For an award of \$2,500.00 to Plaintiff and each of the Class members, as provided by 18 U.S.C. § 2710(c);
- e) For an order permanently enjoining Defendant from disclosing the Private Viewing Information of its subscribers to third parties in violation of the VPPA;
- f) For prejudgment interest on all amounts awarded; and
- g) For an order awarding punitive damages, reasonable attorneys' fees, and costs to counsel for Plaintiff and the Class under Rule 23 and 18 U.S.C. § 2710(c).

Respectfully submitted,

Dated: September 20, 2024

HEDIN LLP

/s/ Elliot O. Jackson

Elliot O. Jackson

NY Attorney Reg. No. (6076798)

HEDIN LLP

1395 Brickell Ave., Suite 610

Miami, Florida 33131-3302

Telephone: (305) 357-2107

Facsimile: (305) 200-8801

ejackson@hedinllp.com

Tyler K. Somes*

District of Columbia Bar No. 90013925

HEDIN LLP

1100 15th Street NW, Ste 04-108

Washington, D.C. 20005

Telephone: (202) 900-3332

Facsimile: (305) 200-8801

tsomes@hedinllp.com

Counsel for Plaintiff and Putative Class

** Pro Hac Vice Application Forthcoming*